

Data Protection Code for Employment Records

The Employment Practices Data Protection Code of Practice governs how employers make use of personal data throughout the employment relationship. Part II of the code, entitled “*Records Management*”, gives guidance on dealing with employment records. This covers records about job applicants (whether successful or not), employees, agency workers, casual workers and contract workers (in each case, irrespective of whether or not they are still working). Some parts of the code may also apply to volunteers and those on work placement.

There is no legal requirement to comply with the Code. However by doing so, employers will ensure they comply with the Data Protection Act 1998 breach of which, in some cases, can lead to a criminal offence. Employers may have alternative ways of meeting the legal requirements of the Act but to do nothing is not an option. Relevant parts of the Code may also be cited by the Information Commissioner in enforcement proceedings under the Act.

The Code contains a series of benchmarks and easy to follow checklist highlighting the procedures to be followed by employers. The recurring theme of the Code is the need to inform workers of the information being held and to use the information only for those purposes of which the workers have been made aware. Some key provisions are highlighted below:

Disclosure of records

The 1998 Act gives all data subjects, including workers, the right to access their personal data and receive a hard copy of it. The Code recommends establishing a policy to ensure such a 'subject access request' is dealt with properly, including notifying other employees if information relating to them will be released in the course of giving access. It also reiterates prospective workers' rights to access their interview notes and references.

Employers should have a policy to cover requests from third parties for disclosure of worker details. Unless under a legal obligation to do so, worker information should only be disclosed if it is fair in the circumstances to do so (the duty of fairness being owed primarily to the worker).

Sickness and accident records

A distinction is made between "absence records" (which may state that the absence is due

to sickness without giving details of the sickness) and "sickness records" (which provide details of the sickness). Unless there is a legitimate need for details of the sickness to be accessed, employers and other employees should not access sickness records. Absence or sickness data for identifiable individuals should not be disclosed to other workers with the exception of managers investigating an individual's absence record.

Fraud Detection

Data matching is a major way in which local authorities now detect fraud. The Code states that trade unions should be consulted before starting such an exercise. Any legitimate concerns raised should be acted before starting the exercise. All workers should be informed of the use of payroll or other data in fraud prevention exercises and they should be reminded of this periodically.

Employers should not disclose worker data to other organisations for the prevention or detection of fraud unless they are required by law to make the disclosure, or they believe that failure to disclose, in a particular instance, is likely to prejudice the prevention or detection of crime, or the disclosure is provided for in workers' contracts of employment

Discipline and grievance

During a disciplinary investigation, there may be a great temptation for an employer to access information it keeps about workers merely because it might assist the employers case. Employers should not do so if this would be incompatible with the purposes for which the information was obtained or disproportionate to the seriousness of the matter being investigated. Employers should state clearly how 'spent' warnings are handled for future disciplinary incidents. The reason for any dismissal of a worker should be properly recorded.

Security

The need to ensure security is reiterated throughout the Code. Whether in paper or electronic form, workers' personal information should be stored safely and access should be restricted to those who have a legitimate business need to know. Background checks, training and confidentiality agreements should all be put into place to ensure the reliability of those who have access to employee data.

The above are just some of the key provisions. All employers are advised to read the whole document. Part 3 of the Code (on monitoring at work) is expected soon and Part 4 (on medical information) two months after that.

It is clear that managers will need to spend some time ensuring the maintenance of up to date and accurate employment records. The Code recommends that a person within the organisation is given the responsibility for ensuring that employment practices and procedures comply with the Act and for ensuring that they continue to do so.

Ibrahim Hasan is Principal Solicitor at Calderdale Council and a training consultant with www.actnowtraining.co.uk